IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF **WHITE MOBILE HOME TRAILER LOCATED BEHIND THE PRIMARY DWELLING AT 15600 COUNTY ROAD 7, MONTPELIER, OHIO 43543, THE PERSON OF RANDY LEE KIRKENDALL, JUNIOR; AND ANY ELECTRONIC DEVICES AND/OR CELLPHONES LOCATED THEREIN/ THEREON, DESCRIBED IN ATTACHMENT A.**	)	CASE NO.: 3:23MJ5167 MAGISTRATE JUDGE DARRELL A. CLAY TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZURE WARRANT

I, James S. Chandler, a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), (hereinafter Affiant) being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. As a Task Force Officer (TFO) of the FBI, I an investigative or law enforcement officer of the United States within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure. Your Affiant is engaged in the enforcement of criminal laws and is within a category of officers authorized by the Attorney General to request and execute search warrants pursuant to Title 18 U.S.C. §§ 3052 and 3107; and DOJ regulations set forth at Title 28 C.F.R. §§ 0.85 and 60.2(a).

2. In October of 2006, this affiant was hired as a Police Officer with the Tiffin Police Department. In June of 2014, this affiant was assigned to the Detective Division of the Tiffin Police Department, and my duties and responsibilities require that this affiant investigate

all types of misdemeanors and felony offenses, including attempted murder, robberies, burglaries, sex crimes, drug investigations, thefts, and receiving stolen property offenses. This affiant has received specialized training and experience in investigations and various forms of criminal offenses. Your affiant has executed search warrants in those cases that have resulted in the discovery and confiscation of evidence, which in turn led to the arrests and convictions of persons involved in criminal behavior. In September of 2020, this affiant was assigned to the Seneca County Drug Task Force/METRICH where this affiant attended numerous drug training courses.

3. In August of 2022, this affiant began employment with the Ohio Bureau of Criminal Investigation in the Special Victims / Human Trafficking Unit. In December of 2022, this affiant was assigned to the Federal Bureau of Investigations (FBI) Child Exploitation and Human Trafficking Task Force as a Task Force Officer (TFO): Job duties include to investigate various crimes ranging from human trafficking to sex crimes related to children.

4. Furthermore, while being employed as a Special Agent with the Bureau of Criminal Investigation and as a Task Force Officer with the Federal Bureau of Investigation Child Exploitation and Human Trafficking Task Force the following facts and information became known to me.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

6. I know that Title 18, United States Code, Section 2252 makes it a crime to distribute, receive, or possess material depicting the sexual exploitation of a minor. I also know that Title 18, United States Code, Section 1466A makes it a crime to knowingly produce,

distribute, receive, or possess with intent to transfer or distribute visual representations which depict minors engaged in sexually explicit conduct and are deemed obscene.

7. Through my experience and training, I am aware that Title 18, United States Code, Section 2256 defines "minor," for purposes of Sections 2252 and 1466A, as "any person under the age of eighteen years." Section 2256 also defines "sexually explicit conduct" for purposes of these sections as including: (a) genital-genital, oral-genital, anal-genital, and oral-anal sexual intercourse, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

8. I am investigating Randy Lee KIRKENDALL Jr., born October 20, 1983. Based on my training and experience and the facts set forth in this Affidavit, there is probable cause to believe that Randy Lee KIRKENDALL Jr. (hereinafter KIRKENDALL) has committed the offense of the receipt of child pornography in violation of Title 18, United States Code, Section 2252(a)(2) (hereinafter the "TARGET OFFENSE"). Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that fruits, evidence, and instrumentalities, described in Attachment B, of the crime(s) are located on the electronic devices associated with the location described in Attachment A.

DEFINITIONS

9. The following definitions apply to this Affidavit and Attachment B:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

c. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

d. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

e. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

f. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides,

negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

10. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

11. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

12. Child pornographers can transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With digital cameras, the images can be transferred directly onto a computer. A computer can connect to another computer using telephone, cable, or wireless connections. Electronic contact can be made to literally millions of computers around the world.

13. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. At the same time, computers have become increasingly smaller and more compact, allowing for more mobility than just their presence and/or use at home. As such, it is common to find individuals in possession of at least one mobile computer (i.e., a cellular telephone with internet access) on their person at any given time, enabling child pornography activities to occur from virtually anywhere the individual goes, especially for individuals after they leave their residences. Because of the advancement in technology and mobility, these smaller computers (i.e., cellular telephones and other small mobile devices with internet access) afford individuals the ability to commit child pornography and other child exploitation crimes at not only their residence but anywhere those individuals go, and yet be located with evidence of such crimes on their person or in their possession. Because of the smaller, more mobile size of such computers, they can be concealed in pockets on the individual's actual person, separate and apart from the individual's residence.

14. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

15. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

16. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

17. Because search engine platforms and companies like Google monitor their platform and try to eliminate or remove any posted sexually explicit content, child pornographers must seek out, find, receive and distribute child pornography through other applications and programs on the internet. One method to receive, possess, and distribute child pornography on

the Internet is through peer-to-peer file sharing (P2P), which is a method of communication available to Internet users through special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer and conducting a search for files that are currently being shared on the network. Some types of P2P software set up their searches by keyword, after which the results are displayed to the user and the user can then select file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file. The downloaded file is stored in the area previously designated by the user and will remain there until moved or deleted. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel, which means that the user can download more than one file at a time, or parts of one file from more than one source computer at a time.

18. A download of child pornography from the internet, including a P2P file transfer, is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

19. Third party software is available to identify the IP address of the P2P or other computer or program sending the file and to identify if parts of the file came from one or more IP addresses. Such software monitors and logs Internet and local network traffic.

20. BitTorrent, one type of P2P software, sets up its searches by keywords, typically on torrent websites. The website does not contain the actual files being shared, only the file referred to as a ".torrent" file. The user then selects a .torrent file(s), from these results, to download. This .torrent file contains instructions on how a user can download the file(s) referenced in the Torrent. A download of a file or files referenced by this .torrent file(s) is achieved by using a BitTorrent client/program, through a direct connection between the computer requesting the file and the computer(s) sharing the actual file(s).

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

21. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information, and yet the storage devices themselves are becoming increasingly smaller and more compact. Users who want to conceal criminal evidence often store it in random order, with deceptive file names, or with encryption or encrypted containers on the device. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

22. To fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

23. In addition, there is probable cause to believe that any computer, cellular telephone, mobile digital device, digital storage device, or any other computer hardware or software found at SUBJECT PREMISES, described in Section I of Attachment A, are instrumentalities of the Target Offense and should all be seized as such.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

24. Based on Affiant's training, experience, and information from other individuals who specialize in the investigation and study of child pornography offenders, Affiant knows that the following traits and characteristics are generally found to exist and be true in cases involving individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject

of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide. With the increasing mobility of computers, including smart cellular telephones (i.e., with internet access), child pornographers/exploiters are not restricted to the confines of their residence or home computers to seek out, view, possess, receive, or distribute child exploitation and pornography material.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose entirely of their sexually explicit material and may go to great lengths to conceal and protect their illicit material from discovery, theft, and damage.

25. Based on my own experience in investigating computer-facilitated child sexual exploitation crimes, and the experiences of other law enforcement agents with whom I have consulted, Affiant believes that the majority of individuals who collect child pornography via the Internet maintain their collections, increasingly in both online and offline storage media, even as they move from one physical location to another.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

g. **Hash Value:** A hash value is created when a mathematical algorithm is applied to a string of text, a file, or the contents of a hard drive. This returns a string of numbers and letters (hash value) that are similar to a DNA strand for that particular data set. Two identical copies of the same file will return the same hash value. If one file is altered in any way the hash will be different.

h. **IP Address:** The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. **Storage medium:** A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

BIOMETRIC ACCESS TO DEVICES

27. This warrant permits law enforcement to compel KIRKENDALL (but not any other individuals present at the SUBJECT PREMISES at the time of execution of the warrant) to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on

devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the biometric features because they are considered a more convenient way to unlock

a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar

restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any computer devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of KIRKENDALL to the fingerprint scanner of the devices found at the SUBJECT PREMISES; (2) hold the computer devices found at the SUBJECT PREMISES in front of the face of KIRKENDALL and activate the facial recognition feature; and/or (3) hold the computer devices found at the SUBJECT PREMISES in front of the face of KIRKENDALL and activate the iris recognition feature, for the purpose of attempting to unlock the computer devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to request that KIRKENDALL state or otherwise provide the password or any other means that may be used to unlock or access the computer devices. Moreover, the proposed warrant does not authorize law enforcement to KIRKENDALL to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the computer devices.

PROBABLE CAUSE

28. Pursuant to Title 18 U.S.C Section 2258A, Electronic Service Providers (“ESP”) or remote computing services to the public though a means or facility of interstate commerce,

such as the Internet, shall report incidents of apparent violations of child exploitation to the National Center for Missing and Exploited Children's (NCMEC) Cyber Tipline. Such reports typically include the files of the suspect images and/or videos.

29. In and around January 2023, FBI Pittsburgh initiated an investigation into Justin HUGHES after Yahoo Inc, an email-service provider, reported HUGHES' Yahoo account to NCMEC in CyberTipline 142875604. Yahoo Inc reported that this account was observed emailing apparent CSAM to the email account **randyleekirkendalljr@gmail.com**.

30. A search for "**randyleekirkendalljr@gmail.com**" in the Internet Crimes Against Children (ICAC) law enforcement database, which is a repository of CyberTipline Reports reported to law enforcement by NCMEC, revealed that on September 24, 2022, Snapchat reported CyberTipline 135530013 to NCMEC. This CyberTipline from Snapchat reported that on or about September 24, 2022, a Snapchat account registered with the email account **randyleekirkendalljr@gmail.com**, Screen/Username "rlki1983" and date of birth (DOB) xx/xx/1983, utilized the Snapchat infrastructure to upload nine (9) files containing suspected CSAM based upon hash values or "hash matches."

31. Of the nine (9) uploaded files, Snapchat (ESP) categorized five (5) files as "apparent child pornography," three (3) files as "child unclothed," and one file as "child pornography (unconfirmed)." The NCMEC CyberTipline Report states the following about this categorization: "Automated file categorization is based on NCMEC's review of uploaded files OR a 'Hash Match' of one or more uploaded files to visually similar files that were previously viewed and categorized by NCMEC at the time a PDF of this report was generated."

32. Further investigation by FBI Pittsburgh revealed that on December 26, 2022, Yahoo Inc reported in CyberTipline Report 142875604 to NCMEC that on November 28, 2022,

a Yahoo Inc account holder received an email with one attached image file containing apparent CSAM. CyberTipline 142875604 also reported that on December 25, 2022, the same Yahoo account holder sent six emails to another individual with several attached video files and one image file containing apparent CSAM. NCMEC reported this CyberTipline and provided the twenty-six (26) uploaded files to FBI Pittsburgh. On January 13, 2023, an FBI Agent in Pittsburgh spoke to the Yahoo Inc investigator listed in the CyberTipline report and they confirmed that they personally viewed the files and determined the files depict apparent CSAM. As explained below, the Pittsburgh FBI Agent also viewed the files and determined that they depicted CSAM.

33. Additionally, HUGHES' Yahoo Inc email data indicated that on December 25, 2022, HUGHES used his Yahoo account budaruski687@gmail.com to send six emails containing twenty-three (23) video files and one image file depicting apparent CSAM to KIRKENDALL's **randyleekirkendalljr@gmail.com** email account. Descriptions of these files include, but are not limited to:

a. An mp4 video file titled "(Pthc) 6yo Asian Girl Sucking.avi.mp4" which depicted an adult male's penis inserted into the mouth of a six-to-nine-year-old female.

b. An mp4 video file titled "facial2.mp4" which depicted an adult male's penis ejaculating on to a six-to-nine-year-old female's face; and

c. An mp4 video file titled "Toddler Cries During a Fuck (43 Seconds).mpeg" which depicted an adult male penetrating the anus of a prepubescent female with his penis.

34. On January 7, 2023, Yahoo Inc submitted a supplemental CyberTipline to NCMEC after a Yahoo Inc investigator determined that the Yahoo Inc account user reported in

CyberTipline 142875604, Justin HUGHES using Yahoo account budaruski687@gmail.com, was a Registered Sex Offender in Pennsylvania. Supplemental CyberTipline report 150076690 stated that the CSAM reported in CyberTipline 142875604 included "approximately twenty-six (26) images and videos of nude prepubescent children, including toddlers, some of whom are engaged in sexual acts with adults. As previously stated, the FBI Pittsburgh Agent viewed the files and confirmed this is an accurate description of several of the files.

35. A search of Pennsylvania State Police's Meghan's Law Public Report indicated that Justin HUGHES, DOB xx/xx/1980, is a lifetime registered sex offender in Pennsylvania.

36. On January 18, 2023, pursuant to a Grand Jury Subpoena issued that same day, Google provided the following information for the email account **randyleekirkendalljr@gmail.com**: Name: Randy Lee KIRKENDALL JR; Recovery SMS: +14195510834; and listed several payment accounts on file for Google Pay in the name Randy Lee KIRKENDALL JR or Randy KIRKENDALL.

37. On September 24, 2022, Snapchat reported in CyberTipline Report 135530013 to NCMEC that on September 24, 2022, a Snapchat account holder uploaded nine files containing apparent CSAM.[1] Snapchat provided the following information for this Snapchat account: Screen/Username: rlki1983; Email Address: **randyleekirkendalljr@gmail.com**; and Date of Birth: xx/xx/1983.

38. On January 20, 2023, FBI Pittsburgh served an Administrative Subpoena to T-Mobile for IP address "2607:fb90:bb07:9036:9915:85d0:b2cd:7b69 (2022-12-02 01:08:49 Z)", which was associated with CSAM. On January 26, 2023, T-Mobile responded and provided the

[1] Your Affiant did not view the contents of these files to determine whether they contain apparent CSAM.

phone number and device information associated with that IP address. They advised that IP address "2607:fb90:bb07:9036:9915:85d0:b2cd:7b69(2022-12-02 01:08:49 Z)" had phone number 419-572-5965 associated with it. T-Mobile provided the account subscriber, billing, and device information for this phone number: Randy L KIRKENDALL Jr., date of birth: October 20, 1983, address 15600 County Road 7, Montpelier, Ohio 43543 maintained this account from November 3, 2022, and December 21, 2022, when the account was canceled.

39. On January 27, 2023, FBI Pittsburgh served an Administrative Subpoena to Metalink Technologies for IP address 173.241.51.20 (2022-09-24 06:14:22 Z) and IP address 173.241.51.20 (2022-09-24 03:00:42 UTC). On January 30, 2023, Metalink Technologies responded with account information of an identified elder female relative of KIRKENDALL, at the property address where KIRKENDALL resides at 15600 County Road 7, Montpelier, Ohio 43543.

40. An open-source database search for Randy Lee KIRKENDALL JR, DOB xx/xx/1983, indicated that KIRKENDALL is a Registered Sex Offender in Ohio. The database also indicated that KIRKENDALL owns phone number 419-551-0834, which was the Recovery SMS listed for the **randyleekirkendalljr@gmail.com** email account which as discussed herein, received CSAM from Justin HUGHES.

41. On March 10, 2023, your affiant's Toledo FBI office received data pursuant to FBI Pittsburgh's prior Federal Search Warrants on KIRKENDALL's Yahoo and Google accounts. On March 13, 2023, FBI Toledo reviewed the material seized from KIRKENDALL's accounts, and your affiant contends that it contained two (2) pictures of CSAM and 11 videos of CSAM. In addition to CSAM, KIRKENDALL's internet search history revealed search queries which reflect a sexual interest in children. Below are examples of KIRKENDALL's internet

search history: "Young incest", "preteen incest", "young preteen incest", "young preteen lolitas", "young porn videos YouPorn.com", "young porn", "real young incest first time - Extreme porn video - Luxure TV", "4443 little girls undies photos in premium high-res pictures", "naked little girls", "tweeny porn", etc. Furthermore, KIRKENDALL also searched for "Omegle - Talk to Strangers" on December 19, 2022. Your affiant is aware that this website is frequently used by pedophiles to access young children for the purposes of getting them to engage in sexual acts via video chatting. Of note, on October 15, 2022, KIRKENDALL searched for "Cycle of child sexual - links between being a victim and becoming a predator". On this same date, KIRKENDALL also searched for "what is the chances of someone that has been sexually abuse abuses as an adult".

42. Your affiant has reviewed the criminal history for the KIRKENDALL. He has prior convictions for sexually oriented state crimes in both Ohio and Indiana. In 2014, he was convicted of ORC 2905.01 “Kidnapping”, and sentenced to three (3) years; he was convicted of ORC 2907.05A4 “Gross Sexual Imposition – Sexual Motivation – Victim under 13”, and sentenced to two (2) years, and KIRKENDALL was also convicted of ORC 2907.323 “Illegal Use of Minor in Nudity Oriented Material – Sexual Motivation” and sentenced to two (2) years. Furthermore, KIRKENDALL was convicted by the State of Indiana of the state charge of “Child Molesting”, and sentenced to six (6) years, with two (2) years of Probation and two (2) years Suspended.

43. This is not the first occasion the FBI has investigated KIRKENDALL. In a 2005 interview of KIRKENDALL by the Toledo FBI, he admitted that he had downloaded CSAM from Yahoo Messenger. He also received a link to his Yahoo email account, which sent him to a website where he admitted to downloading CSAM. KIRKENDALL also admitted in this 2005

interview, to purchasing a membership to a website where he downloaded videos containing CSAM.

44. In 2005, an FBI computer forensics examiner reviewed electronics obtained from KIRKENDALL through an authorized Search Warrant. The investigating agent located many CSAM image files of known and unknown child victims, and numerous movie clips depicting CSAM. The investigating agent also located 25 text files containing stories of explicit sexual activity involving minors.

45. Your Affiant reviewed multiple additional record databases which show that KIRKENDALL currently resides at SUBJECT PREMISES of **15600 County Road 7, Montpelier, Ohio 43543**. Additionally, writer spoke with KIRKENDALL's assigned Adult Parole Authority Officer. On February 21, 2023, his ODRC/APA Parole Officer conducted a home visit with KIRKENDALL, who principally resides in the mobile home trailer located immediately to the East (behind) the primary residence on the property. The Parole Officer met with KIRKENDALL again on March 1, 2023, and KIRKENDALL maintained that same residence at the SUBJECT PREMISES.

46. SUBJECT PREMISES' main residential dwelling is a single-story, single-family residence. SUBJECT PREMISES contains light colored siding, with dark window shutters with black roof shingles. SUBJECT PREMISES is located at 15600 County Road 7, Montpelier, Ohio 43543. FBI Toledo conducted physical surveillance of the property on March 6, 2023, and the location of the mobile home trailer to the East of the main SUBJECT PREMISES was exactly as described by KIRKENDALL's Parole Officer from his February 21, 2023, home visit.

CONCLUSION

47. Based on the aforementioned information, Affiant submits that there is probable cause to believe that Randy Lee KIRKENDALL Jr., residing at SUBJECT PREMISES is involved in Receipt of Child Pornography, in violation of Title 18 U.S.C. §§ 2252(a)(2) and that there is probable cause to believe that items, fruits, or instrumentalities of the offenses will be located within the white mobile home trailer located behind the SUBJECT PREMISES and on the person of KIRKENDALL, including any electronic devices and/or cellphones. In consideration of the foregoing, Affiant respectfully requests that this Court issue a warrant to search the white mobile home trailer SUBJECT PREMISES, described in Attachment A, Section I, for the items described in Attachment B, Section II.

Respectfully submitted,

James S. Chandler
Task Force Officer (TFO)
Federal Bureau of Investigation

Sworn to via telephone after submission by reliable means pursuant to Crim.R. 4.1 and 41(d)(3) this 27th day of April 2023.

DARRELL A. CLAY
UNITED STATES MAGISTRATE JUDGE